

DISTRIBUTION OF POINTS ON CYCLIC CURVES OVER FINITE FIELDS

PATRICK MEISNER

ABSTRACT. We determine in this paper the distribution of the number of points on the cyclic covers of $\mathbb{P}^1(\mathbb{F}_q)$ with affine models $C : Y^r = F(X)$, where $F(X) \in \mathbb{F}_q[X]$ and r^{th} -power free when q is fixed and the genus, g , tends to infinity. This generalizes the work of Kurlberg and Rudnick and Bucur, David, Feigon and Lalin who considered different families of curves over \mathbb{F}_q . In all cases, the distribution is given by a sum of random variables.

1. INTRODUCTION

For any smooth projective, C , of genus g over a finite field know that

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 - \sum_{j=1}^{2g} \alpha_j(C)$$

where the zeta function of C is

$$Z_C(u) = \frac{\prod_{j=1}^{2g} (1 - u\alpha_j(C))}{(1-q)(1-qu)},$$

and $|\alpha_j(C)| = q^{\frac{1}{2}}$ for $j = 1, \dots, 2g$.

The distribution of $\#C(\mathbb{P}^1(\mathbb{F}_q))$ when C varies over families of curves over \mathbb{F}_q is a classical object of study. For several families of curves over \mathbb{F}_q Katz and Sarnak [3] showed that when the genus is fixed and q tends to infinity,

$$\frac{\sum_{j=1}^{2g} \alpha_j(C)}{\sqrt{q}}$$

is distributed as the trace of a random matrix in the monodromy group of the family.

The distribution of the number points on families of curves over finite fields with q fixed while the genus tends to infinity has been a topic of much research recently. It began with Kurlberg and Rudnick [4] determining the distribution of the number of points of hyperelliptic curves. Hyperelliptic curves are in one-to-one correspondence with Galois extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/2\mathbb{Z}$. Bucur, David, Feigon and Lalin [1],[2] extended this result to smooth projective curves that are in one-to-one correspondence with Galois extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/p\mathbb{Z}$, where p is a prime such that $q \equiv 1 \pmod{p}$. Recently Lorenzo, Milione and Meleleo [5] determined the case for Galois group $(\mathbb{Z}/2\mathbb{Z})^n$. In this paper we determine the case for cyclic Galois groups $\mathbb{Z}/r\mathbb{Z}$ for any $q \equiv 1 \pmod{r}$ where r is not necessarily a prime.

Let $K = \mathbb{F}_q(X)$ and let L be a finite Galois extension of K . Let r be an integer such that $q \equiv 1 \pmod{r}$. Suppose that $\text{Gal}(L/K) = \mathbb{Z}/r\mathbb{Z}$. Then there exists a

unique smooth projective curve over \mathbb{F}_q , C , such that $L \cong K(C)$. Further, C will have an affine model of the form

$$Y^r = \alpha F(X), \quad F \in \mathcal{F}_{(d_1, \dots, d_{r-1})} \subset \mathbb{F}_q[X], \alpha \in \mathbb{F}_q^*$$

where

$$\mathcal{F}_{(d_1, \dots, d_{r-1})} = \{F = f_1 f_2^2 \cdots f_{r-1}^{r-1} : f_i \in \mathbb{F}_q[X] \text{ are monic, square-free, pairwise coprime, and } \deg F_i = d_i \text{ for } 1 \leq i \leq r-1\}.$$

The Riemann-Hurwitz formula (Theorem 7.16 of [6]) tells us that if we let $d = \sum_{i=1}^{r-1} i d_i$, then the genus g of the curve C is given by

$$2g + 2r - 2 = \sum_{i=1}^{r-1} (r - (r, i)) d_i + (r - (r, d))$$

where $(r, i) = \gcd(r, i)$. Define now the following sets

$$\begin{aligned} \mathcal{F}_{(d_1, \dots, d_{r-1})}^j &= \mathcal{F}_{(d_1, \dots, d_{j-1}, \dots, d_{r-1})} \\ \hat{\mathcal{F}}_{(d_1, \dots, d_{r-1})} &= \{\alpha F : F \in \mathcal{F}_{(d_1, \dots, d_{r-1})}, \alpha \in \mathbb{F}_q^*\} \\ \hat{\mathcal{F}}_{(d_1, \dots, d_{r-1})}^j &= \hat{\mathcal{F}}_{(d_1, \dots, d_{j-1}, \dots, d_{r-1})} \\ \mathcal{F}_{[d_1, \dots, d_{r-1}]} &= \mathcal{F}_{(d_1, \dots, d_{r-1})} \cup \bigcup_{j=1}^{r-1} \mathcal{F}_{(d_1, \dots, d_{r-1})}^j \\ \hat{\mathcal{F}}_{[d_1, \dots, d_{r-1}]} &= \hat{\mathcal{F}}_{(d_1, \dots, d_{r-1})} \cup \bigcup_{j=1}^{r-1} \hat{\mathcal{F}}_{(d_1, \dots, d_{r-1})}^j. \end{aligned}$$

If we now restrict the d_i such that $\sum_{i=1}^{r-1} i d_i \equiv 0 \pmod{r}$, then the genus will be invariant over curves with affine models $Y^r = F(x)$ with $F(x) \in \hat{\mathcal{F}}_{[d_1, \dots, d_{r-1}]}$. That is, if we let $\mathcal{H}_{g,r}$ be the set of curves of genus g such that $\text{Gal}(L/K) = \mathbb{Z}/r\mathbb{Z}$, we can write

$$\mathcal{H}_{g,r} = \bigcup_{\substack{\sum_{i=1}^{r-1} i d_i \equiv 0 \pmod{r} \\ \sum_{i=1}^{r-1} (r - (r, i)) d_i = 2g + 2r - 2}} \mathcal{H}^{(d_1, \dots, d_{r-1})}$$

where $\mathcal{H}^{(d_1, \dots, d_{r-1})}$ are the curves with affine models in $\hat{\mathcal{F}}_{[d_1, \dots, d_{r-1}]}$. We will discuss the distribution of points not on the whole of $\mathcal{H}_{g,r}$ but on each $\mathcal{H}^{(d_1, \dots, d_{r-1})}$.

Kurlberg and Rudnick [4] first investigated the distribution of points for hyperelliptic curves ($r = 2$). Bucur, David, Feigon and Lalin [1], [2] then extended this result to the case where $r = p$, a prime. They noted that the number of points on such a curve will be given by the formula

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{i=0}^{p-1} \chi_p^i(F(x)) = q + 1 + \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{i=1}^{p-1} \chi_p^i(F(x)),$$

where χ_p is a primitive character on \mathbb{F}_q of order p . Such a character exists since $q \equiv 1 \pmod{p}$. This will be determined by the value $S_p(F) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_p(F(x))$ which leads to the result

Theorem 1.1 (Theorem 1.1 from [1]). *If q is fixed and $d_1, \dots, d_{p-1} \rightarrow \infty$ then for any $t \in \mathbb{Z}[\zeta_p]$*

$$\frac{|\{F \in \hat{\mathcal{F}}_{[d_1, \dots, d_{r-1}]} : S_p(F) = t\}|}{|\hat{\mathcal{F}}_{[d_1, \dots, d_{r-1}]}|} \sim \text{Prob} \left(\sum_{i=1}^{q+1} X_i = t \right)$$

where the X_i are i.i.d random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{p-1}{q+p-1} \\ \zeta_p^j & \text{with probability } \frac{q}{p(q+p-1)} \end{cases}$$

For general r , we prove in Section 2 a formula for the number of point on the curve with affine model $Y^r = F(X)$. In order to state this formula and our main result, we need some notation.

For $d|r$, define

$$F_{(d)}(X) = \prod_{i=1}^{d-1} \left(\prod_{j=0}^{\frac{r}{d}-1} f_{jd+i}(X) \right)^i = \prod_{i=1}^{r-1} f_i(X)^{i \bmod d}.$$

Notice that we could write an affine model for our curve as $Y^r = F_{(r)}(X)$. Further, the $F_{(d)}(X)$ correspond to the subfield extension of L . That is if we have $K \subset L' \subset L$, then $L' = K(C_d)$, where C_d is a curve with affine model $Y^d = F_{(d)}(X)$ for some $d|r$. Then Lemma 2.1 shows that

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 + \sum_{d|r} \sum_{\substack{i=1 \\ (i,d)=1}}^{d-1} \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_d^i(F_{(d)}(x))$$

where χ_d is a primitive character on \mathbb{F}_q of order d . Again, such a character exists since $d|r$ and we are assuming that $q \equiv 1 \pmod{r}$. Hence if we define

$$S_d(F_{(d)}) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_d(F_{(d)}(x))$$

then the number of points on the curve will be determined by the $S_d(F_{(d)})$ for all $d|r$. This leads us to the main theorem

Theorem 1.2. *Write $r = \prod_{j=1}^n p_j^{t_j}$. If q is fixed, then as $d_1, \dots, d_{r-1} \rightarrow \infty$ for any $M_d \in \mathbb{Z}[\zeta_d]$,*

$$\frac{|\{F \in \hat{\mathcal{F}}_{[d_1, \dots, d_{r-1}]} : S_d(F_{(d)}) = M_d, \forall d|r, d \neq 1\}|}{|\hat{\mathcal{F}}_{[d_1, \dots, d_{r-1}]}|} \sim \text{Prob} \left(\sum_{i=1}^{q+1} X_{d,i} = M_d, \forall d|r, d \neq 1 \right)$$

where $X_{d,i}$ are random variables taking values in $\mu_d \cup \{0\}$ such that

$$\text{Prob}(X_{d,i} = 0) = \frac{r - \frac{r}{d}}{q + r - 1}$$

$$\text{Prob}(X_{d,i} = \epsilon_{d,i} \neq 0) = \frac{q + \frac{r}{d} - 1}{d(q + r - 1)}.$$

Moreover, if $i \neq j$ then $X_{d,i}$ and $X_{d',j}$ are independent for all $d, d'|r$. However, if we fix i , then for all $d|r$

$$X_{d,i} = \prod_{p|d} (X_{p^{v_p(d)}, i})^{\sigma_p} \text{ where } 1 \leq \sigma_p \leq \frac{d}{p^{v_p(d)}} \text{ such that } \sigma_p \equiv (p^{v_p(d)})^{-1} \pmod{\frac{d}{p^{v_p(d)}}}.$$

Further, for all $p|r$ and $1 < s \leq v_p(r)$

$$\text{Prob}(X_{p^s,i} = 0 | X_{p^{s-1},i} = 0) = 1$$

$$\text{Prob}(X_{p^{s-1},i} = \epsilon_{p^s,i}^p | X_{p^s,i} = \epsilon_{p^s,i}) = 1.$$

Finally, if $d|r$ but $d \neq r$ then

$\text{Prob}(X_{p^s,i} = \epsilon_{p^s,i} \neq 0, 1 \leq s \leq v_p(d) \text{ and } X_{p^s,i} = 0, v_p(d) < s \leq v_p(r) \text{ for all } p|r)$

$$= \begin{cases} \frac{\phi(\frac{r}{d})}{d(q+r-1)} & \text{if } \epsilon_{p^{s-1},i} = \epsilon_{p^s,i}^p \text{ for all } p|r, 1 \leq s \leq v_p(d) \\ 0 & \text{otherwise} \end{cases}$$

and, if $d = r$,

$$\text{Prob}(X_{p^s,i} = \epsilon_{p^s,i}, s \leq v_p(r), \text{ for all } p|r) = \begin{cases} \frac{q}{r(q+r-1)} & \text{if } \epsilon_{p^{s-1},i} = \epsilon_{p^s,i}^p, 1 \leq s \leq v_p(r), \text{ for all } p|r \\ 0 & \text{otherwise} \end{cases}.$$

To simplify notation, we will prove this for $r = p^n$ in full detail in Section 4, and present in Section 5 the proof for general r . Section 6 gives a heuristic which corroborates the results of Theorem 1.2.

2. NUMBER OF POINTS ON THE CURVE

Let C be the smooth projective curve over \mathbb{F}_q associated to the field $L = \mathbb{F}_q(X) \left(\sqrt[r]{\alpha f_1(X) f_2^2(X) \dots f_{r-1}^{r-1}(X)} \right)$ where the f_i are monic, squarefree and pairwise coprime and $\alpha \in \mathbb{F}_q^*$. Let us determine the smooth affine models of these curves. We first consider the affine model

$$Y^r = \alpha f_1(X) f_2^2(X) \dots f_{r-1}^{r-1}(X).$$

and investigate the smoothness. For any j such that $(j, r) = 1$ we define

$$F^{(j)} = \alpha^j \prod_{i=1}^{r-1} f_i^{ij \pmod r}.$$

Then $F^{(1)} = F$, $F^j = F^{(j)} H^r$ for some $H \in \mathbb{F}_q[X]$ and $Y^r = F^{(j)}(X)$ is another affine model for the curve C .

If $F(x) \neq 0$ then any of the models will be smooth at x . If $f_i(x) = 0$ for some $x \in \mathbb{F}_q$ and for some i such that $(i, r) = d$ then we can find some j such that $(j, r) = 1$ and $ij \equiv d \pmod r$. Hence $F^{(j)}$ would have a d^{th} root at x and the model $Y^r = F^{(j)}(X)$ would be smooth at x if and only if $d = 1$.

Now, without loss of generality we may assume we have an affine model $Y^r = \alpha F(X)$ such that $f_d(x) = 0$ for some $x \in \mathbb{F}_q$ and $d|r$, $d \neq 1$. Moreover, without loss of generality, we may assume $x = 0$. Blowing-up the curve at $(0, 0)$ then we get the variety defined by

$$(Y^r - \alpha f_1^1(X) f_2^2(X) \dots f_{r-1}^{r-1}(X), Xw - Yz)$$

where w, z are projective coordinates. If $z \neq 0$, then $Y = Xw$ and by writing $f_d(X) = X f'_d(X)$ we get

$$\begin{aligned} 0 &= (Xw)^r - X^d \alpha f_1(X) f_2^2(X) \dots f'_d(X) \dots f_{r-1}^{r-1}(X) \\ &= X^d \left((X^{\frac{r}{d}-1} w^{\frac{r}{d}})^d - \alpha f_1(X) f_2^2(X) \dots f'_d(X) \dots f_{r-1}^{r-1}(X) \right). \end{aligned}$$

If we let $Y' = X^{\frac{r}{d}-1} w^{\frac{r}{d}}$, we get the affine model

$$Y'^d = \alpha f_1(X) f_2^2(X) \dots f_d^d(X) \dots f_{r-1}^{r-1}(X)$$

which is birationally equivalent to

$$Y^d = \alpha \prod_{i=1}^{d-1} \left(\prod_{j=0}^{\frac{r}{d}-1} f_{jd+i}(X) \right)^i := F_{(d)}(X).$$

Now $f_d(X) \nmid F_{(d)}(X)$, hence $F_{(d)}(0) \neq 0$ and the affine model will be smooth at 0. Further note that $F_{(r)}(x) = F(x)$.

Further, if x_{q+1} is the point at infinity then

$$F_{(d)}(x_{q+1}) = \begin{cases} \alpha & F \in \mathcal{F}_{(d_1, \dots, d_{r-1})}^{jd}, 1 \leq j \leq r/d - 1 \\ 0 & \text{otherwise} \end{cases}.$$

This leads to the following lemma

Lemma 2.1. *Let C be the smooth projective curve associated to the field $L = \mathbb{F}_q(X) \left(\sqrt[r]{f_1(X) f_2^2(X) \dots f_{r-1}^{r-1}(X)} \right)$ then*

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 + \sum_{d|r} \sum_{\substack{i=1 \\ (i,d)=1}}^{d-1} \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_d^i(F_{(d)}(x)).$$

Proof. If x is not a root of any of the f_i , then there will be r points lying over x , if $F_{(r)}(x)$ is an r^{th} power and no points otherwise. We can write this as

$$1 + \sum_{i=1}^{r-1} \chi_r(F_{(r)}^i(x)) = 1 + \sum_{d|r} \sum_{\substack{i=1 \\ (i,d)=1}}^{d-1} \chi_d^i(F_{(d)}(x)).$$

If $f_i(x) = 0$ for some $(i, r) = 1$, then there will be one point lying over x . Further in this case $F_d(x) = 0$ for all $d|r$ so we can write this as

$$1 + \sum_{d|r} \sum_{\substack{i=1 \\ (i,d)=1}}^{d-1} \chi_d^i(F_{(d)}(x)).$$

If $f_i(x) = 0$ for some $(i, r) = d \neq 1$, then we have to look at the smooth model $y^d = F_{(d)}(x)$. Thus there will be d points lying over x if $F_{(d)}(x)$ is a d^{th} power and no points otherwise. We can write this as

$$1 + \sum_{i=1}^d \chi_d(F_{(d)}^i(x)) = 1 + \sum_{d'|d} \sum_{\substack{i=1 \\ (i,d')=1}}^{d'-1} \chi_{d'}^i(F_{(d')}^i(x)).$$

Further for any $d'|r$ such that $d' \nmid d$ we get that the exponent of f_i in $F_{(d')}$ is non-zero. Hence $F_{(d')}(x) = 0$. Therefore, regardless of the behavior at x , the number of points lying above x is

$$1 + \sum_{d|r} \sum_{\substack{i=1 \\ (i,d)=1}}^{d-1} \chi_d^i(F_{(d)}(x)).$$

Summing up over all x , we find that

$$\begin{aligned} \#C(\mathbb{F}_q) &= \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \left(1 + \sum_{d|r} \sum_{\substack{i=1 \\ (i,d)=1}}^{d-1} \chi_d^i(F_{(d)}(x)) \right) \\ &= q + 1 + \sum_{d|r} \sum_{\substack{i=1 \\ (i,d)=1}}^{d-1} \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_d^i(F_{(d)}(x)). \end{aligned}$$

□

3. SET COUNT

First we need two lemmas from other papers. The first one is Lemma 6.4 from [5] saying

Lemma 3.1 (Lemma 6.4 from [5]). *Let d_1, \dots, d_n be positive integers. For $0 \leq \ell \leq q$ let x_1, \dots, x_ℓ be distinct elements of \mathbb{F}_q . Let $U \in \mathbb{F}_q[x]$ be such that $U(x_i) \neq 0$ for $1 \leq i \leq \ell$. Let $a_{1,1}, \dots, a_{\ell,1}, \dots, a_{1,n}, \dots, a_{\ell,n} \in \mathbb{F}_q^*$. Then the size of $\{(f_1, \dots, f_n) \in \mathcal{F}_{d_1} \times \dots \times \mathcal{F}_{d_n} : (f_i, f_j) = (f_i, U) = 1, f_j(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\}$ is*

$$R_n^U(\ell) := \frac{L_{n-1} q^{d_1 + \dots + d_n}}{\zeta_q^n(2)} \left(\frac{q}{(q-1)^n(q+n)} \right)^\ell \prod_{P|U} \frac{|P|}{|P|+n} \left(1 + O\left(q^{-\frac{\min d_i}{2}}\right) \right)$$

where

$$L_n = \prod_{j=1}^n K_j$$

and

$$K_j = \prod_P \left(1 - \frac{j}{(|P|+1)(|P|+j)} \right).$$

From now on, if K_j or L_n appears elsewhere in the paper, it will be the same formula that appears in the above Lemma 3.1. The next lemma is Lemma 3.2 from [1]

Lemma 3.2 (Lemma 3.2 from [1]). *Fix $x_1, \dots, x_\ell \in \mathbb{F}_q$ and let U be a polynomial of degree u with $U(x_i) \neq 0$, $1 \leq i \leq \ell$. Define the multiplicative function*

$$c_j^U(F) = \begin{cases} \mu^2(F) \prod_{P|F} (1 + j|P|^{-1})^{-1} & F(x_i) \neq 0, 1 \leq i \leq \ell, (F, U) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then for any $0 < \epsilon < 1$

$$\sum_{\deg(F)=d} c_j^U(F) = \frac{K_j q^d}{\zeta_q(2)} \left(\frac{q+j}{q+j+1} \right)^\ell \left(\prod_{P|U} \left(\frac{|P|+j}{|P|+j+1} \right) \right) \left(1 + O\left(q^{\epsilon(d+u+\ell)-d}\right) \right).$$

We use these two lemmas to prove the following lemma.

Lemma 3.3. *Let $d_{1,1}, \dots, d_{r_1-1,1}, \dots, d_{1,n}, \dots, d_{r_n-1,n}$ be positive integers. For $0 \leq \ell \leq q$ let x_1, \dots, x_ℓ be distinct elements of \mathbb{F}_q . Let $U \in \mathbb{F}_q[x]$ be such that $U(x_i) \neq 0$ for $1 \leq i \leq \ell$. Let $a_{1,1}, \dots, a_{\ell,1}, \dots, a_{1,n}, \dots, a_{\ell,n} \in \mathbb{F}_q^*$. Then the size of*

$$\{(F_1, \dots, F_n) \in \mathcal{F}_{d_{1,1}, \dots, d_{r_1-1,1}} \times \dots \times \mathcal{F}_{d_{1,n}, \dots, d_{r_n-1,n}} : (F_j, F_k) = (F_j, U) = 1, F_j(x_i) = a_{i,j}, \\ 1 \leq i \leq \ell, 1 \leq j, k \leq n, j \neq k\}$$

is

$$T_n^U(\ell) := \frac{L_{r_1+\dots+r_n-n-1} q^{d_{1,1}+\dots+d_{r_n-1,n}}}{\zeta_q(2)^{r_1+\dots+r_n-n}} \left(\frac{q}{(q-1)^n(q+r_1+\dots+r_n-n)} \right)^\ell \\ \times \prod_{P|U} \frac{|P|}{|P|+r_1+\dots+r_n-n} \left(1 + O\left(q^{-\frac{\min d_{i,j}}{2}}\right) \right).$$

Proof. If we write $F_i = \prod_{j=1}^{r_i-1} f_{i,j}^j$ then,

$$T_n^U(\ell) = \sum_{\substack{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1 \\ (f_{i,j}, f_{k,h})=1 \\ f_{i,j}(x_m) \neq 0}} R_n^{U \prod_{j \neq 1} f_{i,j}}(\ell) \\ = \sum_{\substack{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1 \\ (f_{i,j}, f_{k,h})=1 \\ f_{i,j}(x_m) \neq 0}} \frac{L_{n-1} q^{d_{1,1}+\dots+d_{1,n}}}{\zeta_q^n(2)} \left(\frac{q}{(q-1)^n(q+n)} \right)^\ell \prod_{P|U \prod_{j \neq 1} f_{i,j}} \frac{|P|}{|P|+n} \left(1 + O\left(q^{-\frac{\min d_{1,j}}{2}}\right) \right) \\ = \frac{L_{n-1} q^{d_{1,1}+\dots+d_{1,n}}}{\zeta_q^n(2)} \left(\frac{q}{(q-1)^n(q+n)} \right)^\ell \left(1 + O\left(q^{-\frac{\min d_{1,j}}{2}}\right) \right) \sum_{\substack{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1 \\ (f_{i,j}, f_{k,h})=1 \\ f_{i,j}(x_m) \neq 0}} \prod_{P|U \prod_{j \neq 1} f_{i,j}} \frac{|P|}{|P|+n}.$$

Lemma 3.2 shows that

$$\sum_{\substack{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1 \\ (f_{i,j}, f_{k,h})=1 \\ f_{i,j}(x_m) \neq 0}} \prod_{P|U \prod_{j \neq 1} f_{i,j}} \frac{|P|}{|P|+n} = \sum_{\deg(f_{2,1})=d_{2,1}} c_n^U(f_{2,1}) \sum_{\deg(f_{2,2})=d_{2,2}} c_n^{U f_{2,1}}(f_{2,2}) \dots \\ \sum_{\deg(f_{r_n-1,n})=d_{r_n-1,n}} c_n^{U \prod_{i \neq 1} f_{i,j}}(f_{r_n-1,n})$$

$$= \frac{L_{r_1+\dots+r_n-n-1} q^{d_{1,1}+\dots+d_{r_n-1,n}}}{\zeta_q(2)^{r_1+\dots+r_n-n}} \left(\frac{q}{(q-1)^n(q+r_1+\dots+r_n-n)} \right)^\ell \\ \times \prod_{P|U} \frac{|P|}{|P|+r_1+\dots+r_n-n} \left(1 + O\left(q^{-\epsilon \min d_{i,j}}\right) \right).$$

Thus, for an appropriate choice of ϵ , we get the result. \square

Lemma 3.3 deals with the case where the F_i are all coprime. We want, however the case where they are not necessarily coprime. Suppose now that we have

$(F_1, \dots, F_n) \in \mathcal{F}_{d_{1,1}, \dots, d_{r_1-1,1}} \times \dots \times \mathcal{F}_{d_{1,n}, \dots, d_{r_n-1,n}}$ which are not necessarily coprime. Let

$$F_j = \prod_{k=1}^{r_j-1} f_{j,k}^k.$$

and we want to rewrite the F_j as products of square-free polynomials that are all coprime to one another. For example, if $n = 2, r_1 = r_2 = 4$ then we would have

$$F_1 = f_{1,1}f_{1,2}^2f_{1,3}^3 \quad F_2 = f_{2,1}f_{2,2}^2f_{2,3}^3.$$

Then if we define

$$f_{(i,j)} = \gcd(f_{1,i}, f_{2,j}), 1 \leq i, j \leq 3$$

and

$$f_{(i,0)} = \frac{f_{1,i}}{f_{(i,1)}f_{(i,2)}f_{(i,3)}} \quad f_{(0,j)} = \frac{f_{2,j}}{f_{(1,j)}f_{(2,j)}f_{(3,j)}}, 1 \leq i, j \leq 3.$$

Then we can all the $f_{(i,j)}$ are square-free and coprime to one another. Moreover

$$F_1 = f_{(1,0)}f_{(1,1)}f_{(1,2)}f_{(1,3)}f_{(2,0)}^2f_{(2,1)}^2f_{(2,2)}^2f_{(2,3)}^2f_{(3,0)}^3f_{(3,1)}^3f_{(3,2)}^3f_{(3,3)}^3 = \prod_{\substack{i=0 \\ (i,j) \neq (0,0)}}^3 \prod_{j=0}^3 f_{(i,j)}^i$$

$$F_2 = f_{(0,1)}f_{(0,2)}f_{(0,3)}f_{(1,0)}f_{(1,1)}f_{(1,2)}f_{(1,3)}f_{(2,0)}^2f_{(2,1)}^2f_{(2,2)}^2f_{(2,3)}^2f_{(3,0)}^3f_{(3,1)}^3f_{(3,2)}^3f_{(3,3)}^3 = \prod_{\substack{i=0 \\ (i,j) \neq (0,0)}}^3 \prod_{j=0}^3 f_{(i,j)}^j.$$

In general, define

$$\mathcal{R} = [0, \dots, r_1 - 1] \times \dots \times [0, \dots, r_n - 1] \setminus \{(0, 0, \dots, 0)\}$$

and write $\vec{\alpha} \in \mathcal{R}$ as $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$. Define also $f_{\vec{\alpha}}$ to be the largest polynomial such that

$$f_{\vec{\alpha}} \text{ divides } \gcd_{\substack{j=1, \dots, n \\ \alpha_j \neq 0}} (f_{j, \alpha_j}) \quad \text{and} \quad (f_{\vec{\alpha}}, \prod_{\substack{j=1 \\ \alpha_j=0}}^n F_j) = 1.$$

With this definition we get if $\vec{\alpha} \neq \vec{\beta}$ then $(f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1$. Indeed, suppose we have $\alpha_j \neq \beta_j$ and $\alpha_j, \beta_j \neq 0$. Then $f_{\vec{\alpha}} | f_{j, \alpha_j}$ and $f_{\vec{\beta}} | f_{j, \beta_j}$ and since $(f_{j, \alpha_j}, f_{j, \beta_j}) = 1$, we get that $(f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1$. On the other hand suppose we have $\alpha_j \neq \beta_j = 0$. Then $f_{\vec{\alpha}} | f_{j, \alpha_j} | F_j$ but $(f_{\vec{\beta}}, F_j) = 1$ hence $(f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1$.

Now, define $\vec{\beta} = (0, \dots, 0, k, 0, \dots, 0)$, where the k is in the j^{th} position. Then $f_{\vec{\beta}}$ is the largest polynomial that divides $f_{j,k}$ that is coprime to all the other $f_{j',k'}$. If $f_{\vec{\beta}} \neq f_{j,k}$ then

$$\prod_{\substack{\vec{\alpha} \neq \vec{\beta} \\ \alpha_j = k}} f_{\vec{\alpha}}$$

is the largest polynomial that divides $f_{j,k}$ that is not coprime to at least one of the other $f_{j',k'}$. If $f_{\vec{\beta}} = f_{j,k}$, then $f_{\vec{\alpha}} = 1$ for all $\vec{\alpha} \neq \vec{\beta}$ such that $\alpha_j = k$. In either case we get

$$f_{j,k} = f_{\vec{\beta}} \prod_{\substack{\vec{\alpha} \neq \vec{\beta} \\ \alpha_j = k}} f_{\vec{\alpha}} = \prod_{\alpha_j = k} f_{\vec{\alpha}}.$$

We then rewrite

$$F_j = \prod_{k=1}^{r_j-1} f_{j,k}^k \quad \text{as} \quad F_j = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}.$$

Define $\vec{d}(\vec{\alpha}) := (d(\vec{\alpha}))_{\vec{\alpha} \in \mathcal{R}}$ to be an integer vector with non-negative entries indexed by the vectors of \mathcal{R} . Further, define the set

$$\mathcal{F}_{\vec{d}(\vec{\alpha})} = \{(f_{\vec{\alpha}})_{\vec{\alpha} \in \mathcal{R}} \in \prod_{\vec{\alpha} \in \mathcal{R}} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \text{ for all } \vec{\alpha} \neq \vec{\beta} \in \mathcal{R}\}.$$

To ease notation, we will write just $(f_{\vec{\alpha}})$ instead of $(f_{\vec{\alpha}})_{\vec{\alpha} \in \mathcal{R}}$ if it is clear what set the indices $\vec{\alpha}$ run over. Hence,

$$\begin{aligned} & \{(F_1, \dots, F_n) \in \mathcal{F}_{d_{1,1}, \dots, d_{r_1-1,1}} \times \dots \times \mathcal{F}_{d_{1,n}, \dots, d_{r_n-1,n}} : F_j(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\} \\ &= \bigcup_{\substack{\vec{d}(\vec{\alpha}) \\ \sum_{\alpha_j=k} d(\vec{\alpha})=d_{j,k}}} \{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\} \end{aligned}$$

This leads to Proposition 3.4

Proposition 3.4. *Let $\vec{d}(\vec{\alpha})$ be as above. For $0 \leq \ell \leq q$ let x_1, \dots, x_{ℓ} be distinct elements of \mathbb{F}_q . Let $a_{1,1}, \dots, a_{\ell,1}, \dots, a_{1,n}, \dots, a_{\ell,n} \in \mathbb{F}_q^*$. Then the size of*

$$\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_j(x_i) := \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\}$$

is

$$S_n(\ell) := \frac{L_{r_1 \dots r_n - 2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}}{\zeta_q(2)^{r_1 \dots r_n - 1}} \left(\frac{q}{(q-1)^n (q + r_1 \dots r_n - 1)} \right)^{\ell} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}{2}}\right) \right).$$

Proof. We will split the $F_j := \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}$ into their coprime parts. In order to do this we will need some new notation. Define

$$\mathcal{S}_j := \{(0, \dots, 0, \alpha_j, 0, \dots, 0) : 1 \leq \alpha_j \leq r_j - 1\} \subset \mathcal{R}$$

where the non-zero entry is in the j^{th} coordinate. Define,

$$\mathcal{S} = \bigcup_{j=1}^n \mathcal{S}_j.$$

Then the factor of $F_j = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}$ that is coprime to all F_i such that $i \neq j$ will be $\prod_{\vec{\alpha} \in \mathcal{S}_j} f_{\vec{\alpha}}^{\alpha_j}$. Further for any subset $\mathcal{R}' \subset \mathcal{R}$, define

$$\mathcal{F}_{(\vec{d}(\vec{\alpha}))_{\vec{\alpha} \in \mathcal{R}'}}^{\mathcal{R}'} = \{(f_{\vec{\alpha}}) \in \prod_{\vec{\alpha} \in \mathcal{R}'} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1, \text{ for } \alpha \neq \beta \in \mathcal{R}'\}.$$

We will denote this as just $\mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{R}'}$ with the understanding that in this context $\vec{d}(\vec{\alpha})$ is indexed by \mathcal{R}' instead of \mathcal{R} . Then,

$$\begin{aligned}
S_n(\ell) &= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\}| \\
&= \sum_{\substack{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{R} \setminus \mathcal{S}} \\ f_{\vec{\alpha}}(x_i) \neq 0}} |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{S}} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1, \vec{\alpha} \in \mathcal{S}, \vec{\beta} \in \mathcal{R} \setminus \mathcal{S} \prod_{\vec{\alpha} \in \mathcal{S}_j} f_{\vec{\alpha}}^{\alpha_j}(x_i) = b_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\
&= \sum_{\substack{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{R} \setminus \mathcal{S}} \\ f_{\vec{\alpha}}(x_i) \neq 0}} T_n^{\prod_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} f_{\vec{\alpha}}}(\ell)
\end{aligned}$$

where $T_n^{\prod_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} f_{\vec{\alpha}}}(\ell)$ is as in Lemma 3.3 and

$$b_{i,j} = a_{i,j} \prod_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} f_{\vec{\alpha}}(x_i)^{-\alpha_j}.$$

Thus, similarly to the previous lemma,

$$\begin{aligned}
S_n(\ell) &= \sum_{\substack{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{R} \setminus \mathcal{S}} \\ f_{\vec{\alpha}}(x_i) \neq 0}} \frac{L_{r_1+\dots+r_n-n-1} q^{\sum_{\vec{\alpha} \in \mathcal{S}} \vec{d}(\vec{\alpha})}}{\zeta_q(2)^{r_1+\dots+r_n-n}} \left(\frac{q}{(q-1)^n (q+r_1+\dots+r_n-n)} \right)^\ell \\
&\times \prod_{\substack{P|f_{\vec{\alpha}} \\ \vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}}} \frac{|P|}{|P|+r_1+\dots+r_n-n} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{S}} d_{\vec{\alpha}}}{2}}\right) \right) \\
&= M \frac{L_{r_1+\dots+r_n-n-1} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}}{\zeta_q(2)^{r_1+\dots+r_n-n}} \left(\frac{q}{(q-1)^n (q+r_1+\dots+r_n-n)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{S}} d_{\vec{\alpha}}}{2}}\right) \right).
\end{aligned}$$

By the same reasoning as in the proof of Lemma 3.3 we get

$$\begin{aligned}
M &= \sum_{\substack{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{R} \setminus \mathcal{S}} \\ f_{\vec{\alpha}}(x_i) \neq 0}} \prod_{\substack{P|f_{\vec{\alpha}} \\ \vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}}} \frac{|P|}{|P|+r_1+\dots+r_n-n} \\
&= \frac{L_{r_1\dots r_n-1} q^{\sum_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} d_{\vec{\alpha}}}}{L_{r_1+\dots+r_n-n-1} \zeta_q(2)^{r_1\dots r_n-r_1-\dots-r_n+n-1}} \left(\frac{q+r_1+\dots+r_n-n-1}{q+r_1\dots r_n-1} \right)^\ell \left(1 + O\left(q^{-\epsilon \min_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} d_{\vec{\alpha}}}\right) \right).
\end{aligned}$$

Therefore, if we choose an appropriate ϵ , we get the result. \square

4. THE CASE $r = p^n$

In order to apply the counting formula of Proposition 3.4 we want to write the n functions defined by

$$F_{(p^j)}(X) = \prod_{i=1}^{p^n-1} f_i^i \pmod{p^j} \quad 1 \leq j \leq n$$

in terms of coprime functions.

To apply the results of Section 3 we define, in this context

$$\mathcal{R} = [0, \dots, p-1]^n \setminus \{(0, \dots, 0)\}.$$

If $\vec{\alpha} \in \mathcal{R}$ we will denote it $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$. Rewrite

$$F := \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_1 + p\alpha_2 + \dots + p^{n-1}\alpha_n}.$$

That is we make the identification $f_{\alpha_1 + p\alpha_2 + \dots + p^{n-1}\alpha_n} \rightarrow f_{(\alpha_1, \dots, \alpha_n)}$

Recall the notation in Section 2 where we denoted, for $d|r$,

$$F_{(d)}(X) := \prod_{i=1}^{d-1} \left(\prod_{j=0}^{\frac{r}{d}-1} f_{jd+i}(X) \right)^i = \prod_{i=1}^{r-1} f_i(X)^i \pmod{d}.$$

and we have

$$F_{(p^j)}(X) = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}(X)^{\alpha_1 + p\alpha_2 + \dots + p^{j-1}\alpha_j}$$

for $j = 1, \dots, n$. Further, if necessary, we denote $F_{(1)}(X) = 1$.

Define $d_1 := d(1, 0, \dots, 0)$. Also use the notation $f_1 = f_{(1,0,\dots,0)}$. We will redefine the sets in Section 1 using this new notation.

$$\mathcal{R}' = \mathcal{R} \setminus \{(1, 0, \dots, 0)\}$$

$$\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})} = \{(f_1, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{d_1} \times \prod_{\vec{\alpha} \in \mathcal{R}'} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \text{ for all } \vec{\alpha} \neq \vec{\beta}\}$$

Let

$$\delta(\vec{\alpha}, \vec{\beta}) = \begin{cases} 1 & \vec{\alpha} = \vec{\beta} \\ 0 & \vec{\alpha} \neq \vec{\beta} \end{cases}.$$

Then define

$$\mathcal{F}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}} = \{(f_{\vec{\beta}}, (f_{\vec{\alpha}})) \in \mathcal{F}_{d(\vec{\beta})-1} \times \prod_{\vec{\alpha} \neq \vec{\beta}} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\gamma}}) = 1, \vec{\alpha} \neq \vec{\gamma} \in \mathcal{R}\}.$$

Likewise define $\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}}$ to be elements of $\mathcal{F}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}}$ where f_1 is not necessarily monic.

Further, define

$$\begin{aligned} \mathcal{F}_{[\vec{d}(\vec{\alpha})]} &= \mathcal{F}_{\vec{d}(\vec{\alpha})} \cup \bigcup_{\vec{\beta} \in \mathcal{R}} \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}} \\ \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} &= \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})} \cup \bigcup_{\vec{\beta} \in \mathcal{R}} \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}}. \end{aligned}$$

Now, if x_{q+1} is the point at infinity, then,

$$F_{(p^j)}(x_{q+1}) = \begin{cases} \text{leading coefficient of } f_1 & (f_{\vec{\alpha}}) \in \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}} \\ 0 & \text{otherwise} \end{cases}$$

where $\vec{\beta} = (\beta_1, \dots, \beta_n) \in \mathcal{R}$ is any tuple such that $\beta_i = 0$ for all $i \leq j$.

Proposition 4.1. *Let $a_{i,j} \in \mathbb{F}_q^*$, $1 \leq j \leq n$, $1 \leq i \leq \ell$ such that $a_{i,j} = a_{i,j-1}(b_{i,j})^{p^{j-1}}$ for some $b_{i,j} \in \mathbb{F}_q^*$. We let $a_{i,0} = 1$ so that $a_{i,1} = b_{i,1}$. Then*

$$\begin{aligned} & |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p^j)}(x_i) = a_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\ &= \frac{L_{p^n-2q} \sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{\zeta_q(2)^{p^n-1}} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}{2}}\right) \right). \end{aligned}$$

Proof. For $j = 1, \dots, n$ define $F_j = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}$. Then we can write $F_{(p^j)} = F_{(p^{j-1})} F_j^{p^{j-1}}$, where, again, we have $F_1 = 1$. Then $F_{(p^j)}(x_i) = a_{i,j}$ for all i, j is equivalent to $F_j(x_i) = \epsilon_{i,j} b_{i,j}$ for all i, j for some $\epsilon_{i,j} \in \mu_{p^{j-1}}$. Hence,

$$\begin{aligned} & |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p^j)}(x_i) = a_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\ &= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_j(x_i) = \epsilon_{i,j} b_{i,j}, \epsilon_{i,j} \in \mu_{p^{j-1}}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\ &= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right). \end{aligned}$$

Where the second equality comes from Proposition 3.4 and that there are $(p^{\frac{n(n-1)}{2}})^\ell$ different choices for the $\epsilon_{i,j}$. \square

Now let us look at what happens if some of the $a_{i,j} = 0$. Note that if $a_{i,j} = 0$ then $a_{i,j+1} = 0$ as $F_{p^j} | F_{p^{j+1}}$. Thus we have

Corollary 4.2. *Let $a_{i,j} \in \mathbb{F}_q$, $1 \leq j \leq n$, $1 \leq i \leq \ell$ such that*

$$a_{i,1}, \dots, a_{i,k} \neq 0 \text{ and } a_{i,k+1}, \dots, a_{i,n} = 0 \text{ for } \sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k$$

for $k = 0, \dots, n-1$ and $a_{i,j} \neq 0$ for all j for $\sum_{i=0}^{n-1} m_i + 1 \leq i \leq \ell$. Further, if $a_{i,j} \neq 0$ then $a_{i,j} = a_{i,j-1} (b_{i,j})^{p^{j-1}}$ for some $b_{i,j} \in \mathbb{F}_q^*$. Then

$$\begin{aligned} & |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{p^j}(x_i) = a_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\ &= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-k-1}(q-1)^{n-k}}{qp^{\frac{(n-k)(n+k-1)}{2}}} \right)^{m_k} \\ & \quad \times \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right). \end{aligned}$$

Proof. Consider i such that $\sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k$. Then $f_{\vec{\alpha}}(x_i) = 0$ for some $\vec{\alpha}$ such that $\alpha_{k+1} \neq 0$ but $\alpha_j = 0$ for all $j < k+1$. There are $(p-1)p^{n-j-1}$ different such $\vec{\alpha}$. Fix a partition $m_k := \sum_{\vec{\alpha}} m_{k,\vec{\alpha}}$ where the sum is over all such $\vec{\alpha}$ defined above and $m_{k,\vec{\alpha}}$ is the number of times $f_{\vec{\alpha}}(x_i) = 0$.

Define $f'_{\vec{\alpha}}$ as $f_{\vec{\alpha}}$ divided by its roots and F'_{p^j} as the corresponding product of the $f'_{\vec{\alpha}}$. Now $F'_{p^j}(x_i)$ is determined by $F_{p^j}(x_i)$ for $j \leq k$. $F'_{p^j}(x_i)$ will be fixed, up to a p^{j-1} th root of unity, for $j+1 \leq k \leq n$. Thus we get a factor of

$$\left(\prod_{j=k+1}^n \frac{q-1}{p^{j-1}} \right)^{m_k} = \left(\frac{(q-1)^{n-k}}{p^{\frac{(n-k)(n+k-1)}{2}}} \right)^{m_k}.$$

Summing up over all the partitions of m_k we get

$$\begin{aligned}
& |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{p^j}(x_i) = a_{i,j}, 0 \leq j \leq n, 1 \leq i \leq \ell\}| \\
&= \prod_{k=0}^{n-1} ((p-1)p^{n-k-1})^{m_k} \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha}) - \sum_{k=0}^{n-1} m_k}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(q-1)^{n-j}}{p^{\frac{(n-k)(n+k-1)}{2}}} \right)^{m_k} \\
&\quad \times \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \\
&= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-k-1} (q-1)^{n-k}}{qp^{\frac{(n-k)(n+k-1)}{2}}} \right)^{m_k} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).
\end{aligned}$$

□

Corollary 4.3. *Let $\epsilon_{i,j} \in \mu_{p^j} \cup \{0\}$, $1 \leq j \leq n, 1 \leq i \leq \ell$ such that*

$$\epsilon_{i,1}, \dots, \epsilon_{i,k} \neq 0 \text{ and } \epsilon_{i,k+1}, \dots, \epsilon_i^n = 0 \text{ for } \sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k$$

for $k = 0, \dots, n-1$ and $\epsilon_{i,j} \neq 0$ for all j for $\sum_{i=0}^{n-1} m_i + 1 \leq i \leq \ell$. Further, if $\epsilon_{i,j} \neq 0$ then $\epsilon_{i,j-1} = (\epsilon_{i,j})^p$. Then

$$\begin{aligned}
& |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\
&= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{2n-2k-1}}{q} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).
\end{aligned}$$

Proof. For $k = 1, \dots, n$, $F_{p^k}(x_i) = 0$ for $1 \leq i \leq \sum_{j=0}^{k-1} m_j$, so for $\sum_{j=0}^{k-1} m_j + 1 \leq i \leq \ell$, $F_{p^k}(x_i)$ has $\frac{q-1}{p^k}$ choices. Hence

$$\begin{aligned}
& |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\
&= \prod_{k=1}^n \left(\frac{q-1}{p^k} \right)^{\ell - \sum_{j=0}^{k-1} m_j} \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-k-1} (q-1)^{n-k}}{qp^{\frac{(n-k)(n+k-1)}{2}}} \right)^{m_k} \\
&\quad \times \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \\
&= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{2n-2k-1}}{q} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).
\end{aligned}$$

□

Up until now, we have been looking only at points in \mathbb{F}_q . What we need to look at however, is points in $\mathbb{P}^1(\mathbb{F}_q)$. This is taken care of by the following corollary

Corollary 4.4. *Let $\epsilon_{i,j} \in \mu_{p^j} \cup \{0\}$, $1 \leq j \leq n, 1 \leq i \leq q+1$ such that*

$$\epsilon_{i,1}, \dots, \epsilon_{i,k} \neq 0 \text{ and } \epsilon_{i,k+1}, \dots, \epsilon_{i,n} = 0 \text{ for } \sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k$$

for $k = 0, \dots, n-1$ and $\epsilon_{i,j} \neq 0$ for all j for $\sum_{i=0}^{n-1} m_i + 1 \leq i \leq q+1$. Further, if $\epsilon_{i,j} \neq 0$ then $\epsilon_{i,j-1} = (\epsilon_{i,j})^p$. Then

$$\begin{aligned} & \frac{|\{(f_{\vec{\alpha}}) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q+1\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|} \\ &= \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{2n-2k-1}}{q} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right). \end{aligned}$$

Proof. Case 1: $\epsilon_{q+1,k} \neq 0$ for all $1 \leq k \leq n$.

In this case we get that $(f_{\vec{\alpha}}) \in \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}$. Further the leading coefficient of f_1 under χ_{p^n} must be $\epsilon_{q+1,n}$. Thus

$$\begin{aligned} & \frac{q-1}{p^n} |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q\}| \\ &= \frac{q-1}{p^n} \frac{L_{p^n-2q} \sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{2n-2k-1}}{q} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^q \\ &= \frac{(q-1)(q+p^n-1)}{q} \frac{L_{p^n-2q} \sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{2n-2k-1}}{q} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^{q+1}. \end{aligned}$$

Case 2: $\epsilon_{q+1,1}, \dots, \epsilon_{q+1,k} \neq 0$ and $\epsilon_{q+1,k+1}, \dots, \epsilon_{q+1,n} = 0$ for some k .

In this case we get $(f_{\vec{\alpha}}) \in \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}}$ where $\vec{\beta} = (\beta_1, \dots, \beta_n) \in \mathcal{R}$ such that $\beta_j = 0$ for all $j \leq k$ and $\beta_{k+1} \neq 0$. There are $(p-1)p^{n-k-1}$ such $\vec{\beta}$. Further m_k will go to $m_k - 1$ and the leading coefficient of f_1 under χ_{p^k} must be ϵ_{q+1}^k . Then,

$$\begin{aligned} & \frac{q-1}{p^k} \sum_{\vec{\beta}} |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q\}| \\ &= \frac{q-1}{p^k} (p-1)p^{n-k-1} \frac{L_{p^n-2q} \sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})-1}{\zeta_q(2)^{p^n-1}} \prod_{j=0}^{n-1} \left(\frac{(p-1)p^{2n-2j-1}}{q} \right)^{m_j} \\ & \quad \times \left(\frac{(p-1)p^{2n-2k-1}}{q} \right)^{-1} \left(\frac{q}{p^n(q+p^n-1)} \right)^q \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \\ &= \frac{(q-1)(q+p^n-1)}{q} \frac{L_{p^n-2q} \sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{\zeta_q(2)^{p^n-1}} \prod_{j=0}^{n-1} \left(\frac{(p-1)p^{2n-2j-1}}{q} \right)^{m_j} \\ & \quad \times \left(\frac{q}{p^n(q+p^n-1)} \right)^{q+1} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right). \end{aligned}$$

Thus, independent of the behavior at x_{q+1} , we get our result. \square

Which leads us to restate and prove Theorem 1.2 for $r = p^n$.

Theorem 4.5. Let $M_j \in \mathbb{Z}[\zeta_{p^j}]$ for $j = 1, \dots, n$. Then

$$\frac{|\{(f_{\vec{\alpha}}) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : S_{p^j}(F_{p^j}) = M_j, 1 \leq j \leq n\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \text{Prob} \left(\sum_i X_{i,1} = M_1 \text{ and } \dots \text{ and } \sum_i X_{i,n} = M_n \right) \left(1 + O \left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right)$$

where the $X_{i,j}$ are random variables that take values in $\mu_{p^j} \cup \{0\}$ such that $X_{i,j}$ and $X_{h,k}$ are i.i.d unless $i = h$ and

$$\begin{aligned} \text{Prob}(X_{i,j} = 0) &= \frac{p^n - p^{n-j}}{q + p^n - 1} & \text{Prob}(X_{i,j} = \epsilon_{i,j}) &= \frac{q + p^{n-j} - 1}{p^j(q + p^n - 1)} \\ \text{Prob}(X_{i,j+1} = 0 | X_{i,j} = 0) &= 1 & \text{Prob}(X_{i,j-1} = (X_{i,j})^p | X_{i,j} \neq 0) &= 1 \end{aligned}$$

$$\text{Prob}(X_{i,1} = \epsilon_{i,1}, \dots, X_{i,j} = \epsilon_{i,j} \text{ and } X_{i,j+1}, \dots, X_{i,n} = 0) = \begin{cases} \frac{(p-1)p^{n-2j-1}}{q + p^n - 1} & \epsilon_{i,k-1} = (\epsilon_{i,k})^p, k = 2, \dots, j \\ 0 & \text{otherwise} \end{cases}$$

$$\text{Prob}(X_{i,1} = \epsilon_{i,1}, \dots, X_{i,n} = \epsilon_{i,n}) = \begin{cases} \frac{q}{p^n(q + p^n - 1)} & \epsilon_{i,k-1} = (\epsilon_{i,k})^p, k = 2, \dots, n \\ 0 & \text{otherwise} \end{cases}$$

Proof.

$$\begin{aligned} & \frac{|\{(f_{\vec{\alpha}}) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : S_{p^j}(F_{p^j}) = M_j, 1 \leq j \leq n\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|} \\ &= \sum_{\substack{(E_{1,j}, \dots, E_{q+1,j}) \in \mu_{p^j} \cup \{0\} \\ \sum_i E_{i,j} = M_j \\ E_{i,j} = 0 \implies E_{i,j+1} = 0 \\ E_{i,j} \neq 0 \implies E_{i,j-1} = (E_{i,j})^p \\ j=1, \dots, n}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{2n-2k-1}}{q} \right)^{m_k} \left(\frac{q}{p^n(q + p^n - 1)} \right)^{q+1} \left(1 + O \left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \\ &= \sum_{\substack{(E_{1,j}, \dots, E_{q+1,j}) \in \mu_{p^j} \cup \{0\} \\ \sum_i E_{i,j} = M_j \\ E_{i,j} = 0 \implies E_{i,j+1} = 0 \\ E_{i,j} \neq 0 \implies E_{i,j-1} = (E_{i,j})^p \\ j=1, \dots, n}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2k-1}}{q + p^n - 1} \right)^{m_k} \left(\frac{q}{p^n(q + p^n - 1)} \right)^{q+1-\sum m_k} \left(1 + O \left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \\ &= \text{Prob} \left(\sum_i X_{i,1} = M_1 \text{ and } \dots \text{ and } \sum_i X_{i,n} = M_n \right) \left(1 + O \left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \end{aligned}$$

where the X_i have the desired properties. \square

5. GENERAL r

Suppose now that $r = r_1 r_2$ with $(r_1, r_2) = 1$. Then, relabeling the f_i as $f_{i,j}$ we can write

$$F(X) = \prod_{\substack{i=0, \dots, r_1-1 \\ j=0, \dots, r_2-1 \\ (i,j) \neq (0,0)}} f_{i,j}(X)^{s_2 r_2 i + s_1 r_1 j \mod r}$$

where $s_1 \equiv r_1^{-1} \mod r_2$ and $s_2 \equiv r_2^{-1} \mod r_1$. With this notation we now get

$$F_{r_1} = \prod_{\substack{i=0, \dots, r_1-1 \\ j=0, \dots, r_2-1 \\ (i,j) \neq (0,0)}} f_{i,j}^{i \mod r_1} \quad F_{r_2} = \prod_{\substack{i=0, \dots, r_1-1 \\ j=0, \dots, r_2-1 \\ (i,j) \neq (0,0)}} f_{i,j}^{j \mod r_2}.$$

Therefore

$$F_{r_1}(X)^{s_2 r_2} F_{r_2}(X)^{s_1 r_1} = F(X) \left(\prod_{i,j} f_{i,j}(X)^{n_{i,j}} \right)^r$$

for some, potentially 0, exponents $n_{i,j}$. Further we see that $F(x) = 0$ if and only if $F_{r_1} F_{r_2}(x) = 0$ as all the factors that appear in F appear in $F_{r_1} F_{r_2}$. Therefore the values of $F_d(x)$ for all $d|r$ are determined by the values of $F_{p^n}(x)$ where p is a prime such that $p^n|r$. That is,

$$\begin{aligned} & |\{F \in \mathcal{F}_{(d_1, \dots, d_r)} : \chi_d(F_d(x_i)) = \epsilon_{d,i}, \text{ for all } d|r, 1 \leq i \leq \ell\}| \\ &= |\{F \in \mathcal{F}_{(d_1, \dots, d_r)} : \chi_d(F_d(x_i)) = \epsilon_{d,i}, d = p^n|r, p \text{ a prime}, 1 \leq i \leq \ell\}| \end{aligned}$$

Now, suppose $r = p_1^{t_1} \cdots p_n^{t_n}$. Define

$$\mathcal{R}' = [0, \dots, p_1^{t_1} - 1] \times \cdots \times [0, \dots, p_n^{t_n} - 1] \setminus \{(0, \dots, 0)\}$$

Let

$$\phi : \mathcal{R}' \rightarrow [1, \dots, r - 1]$$

be the isomorphism that comes from the Chinese Remainder Theorem. Then if $F = \prod_{i=1}^{r-1} f_i^i$, we can relabel the f_i to get

$$F = \prod_{\vec{\beta} \in \mathcal{R}'} f_{\vec{\beta}}^{\phi(\vec{\beta})}.$$

Notice that $\phi(\vec{\beta}) \equiv k \pmod{p_j^{t_j}}$ if and only if $\beta_j = k$. Therefore

$$F_{(p_j^{t_j})} = \prod_{\vec{\beta} \in \mathcal{R}'} f_{\vec{\beta}}^{\phi(\vec{\beta})} \pmod{p_j^{t_j}} = \prod_{k=0}^{p_j^{t_j}-1} \prod_{\substack{\beta \in \mathcal{R}' \\ \beta_j = k}} f_{\vec{\beta}}^k = \prod_{\vec{\beta} \in \mathcal{R}'} f_{\vec{\beta}}^{\beta_j}.$$

However, we need all powers of the primes. Therefore we define

$$\mathcal{R} = [0, \dots, p_1 - 1]^{t_1} \times \cdots \times [0, \dots, p_n - 1]^{t_n} \setminus \{(0, \dots, 0)\}.$$

Let $T_j = \sum_{i=1}^j t_i$. As usual, for $\vec{\alpha} \in \mathcal{R}$ we write it as $\vec{\alpha} = (\alpha_1, \dots, \alpha_{T_n})$. Then there is an isomorphism $\psi : \mathcal{R} \rightarrow \mathcal{R}'$ such that

$$\psi(\vec{\alpha}) = (\alpha_1 + p_1 \alpha_2 + \cdots + p_1^{t_1-1} \alpha_{T_1}, \dots, \alpha_{T_{n-1}+1} + p_n \alpha_{T_{n-1}+2} + \cdots + p_n^{t_n-1} \alpha_{T_n})$$

Therefore, if we relabel the $f_{\vec{\beta}}$ we get

$$F_{(p_j^{t_j})}(X) = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_{T_{j-1}+1} + p \alpha_{T_{j-1}+2} + \cdots + p^{t_j-1} \alpha_{T_j}}(X)$$

Moreover, for any $1 \leq k_j \leq t_j$

$$F_{(p_j^{k_j})}(X) = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_{T_{j-1}+1} + p \alpha_{T_{j-1}+2} + \cdots + p^{k_j-1} \alpha_{T_{j-1}+k_j}}(X)$$

Then we get

$$\begin{aligned} & |\{F \in \mathcal{F}_{(d_1, \dots, d_{r-1})} : F_{(p_j^{k_j})}(x_i) = a_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}| \\ &= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i) = a_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}| \end{aligned}$$

where $d(\vec{\alpha}) = d_{\phi \circ \psi(\vec{\alpha})}$.

Proposition 5.1. *Let $a_{i,j,k_j} \in \mathbb{F}_q^*$ such that $a_{i,j,k_j} = a_{i,j,k_j-1}(b_{i,j,k_j})^{p^{k_j-1}}$ for some $b_{i,j,k_j} \in \mathbb{F}_q^*$. Further we let that $a_{i,j,0} = 1$ so that $a_{i,j,1} = b_{i,j,1}$.*

$$\begin{aligned} & |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i) = a_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}| \\ &= \frac{L_{r-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{r-1}} \left(\frac{q \prod_{j=1}^n p^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{T_n}(q+r-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}}\right) \right). \end{aligned}$$

Proof. As we saw in the proof of Proposition 4.1, it will be enough to consider what values the polynomials

$$F_{(j,k_j)} = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_{T_j-1+k_j}}$$

up to some root of unity. That is,

$$\begin{aligned} & |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i) = a_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}| \\ &= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(j,k_j)}(x_i) = \epsilon_{i,j,k_j} b_{i,j,k_j}, \epsilon_{i,j,k_j} \in \mu_{p^{k_j-1}}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}|. \end{aligned}$$

We can define an isomorphism

$$\phi : \{(j, k_j) : 1 \leq j \leq n, 1 \leq k_j \leq T_j\} \rightarrow \{1, \dots, T_n\}$$

by

$$\phi(j, k_j) = T_{j-1} + k_j.$$

Let $\epsilon_{i,j} = \epsilon_{i,\phi^{-1}(j)}$, $\beta_{i,j} = \beta_{i,\phi^{-1}(j)}$ and $F_j = F_{\phi^{-1}(j)}$, then

$$F_j = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}.$$

If we denote $\mu_m = \mu_{p_j^{k_j}}$ where $\phi(j, k_j) = m$ then,

$$\begin{aligned} & |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(j,k_j)}(x_i) = \epsilon_{i,j,k_j} b_{i,j,k_j}, \epsilon_{i,j,k_j} \in \mu_{p_j^{k_j-1}}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}| \\ &= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_j(x_i) = \epsilon_{i,j} b_{i,j}, \epsilon_{i,j} \in \mu_j, 1 \leq j \leq T_n, 1 \leq i \leq \ell\}| \\ &= \frac{L_{r-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{r-1}} \left(\frac{q \prod_{j=1}^n p^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{T_n}(q+r-1)} \right)^\ell \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}}\right) \right) \end{aligned}$$

where the last equality comes from Proposition 3.4. \square

Define

$$\mathcal{S} = [0, \dots, t_1] \times \dots \times [0, \dots, t_n] \setminus (t_1, \dots, t_n).$$

For any $S \in \mathcal{S}$ we will write $S = (s_1, \dots, s_n)$. We will use \mathcal{S} to count the number of $1 \leq i \leq \ell$ such that $F_{(p_j^{k_j})}(x_i) = 0$. That is, for every $S = (s_1, \dots, s_n) \in \mathcal{S}$ we say that for some i $F_{(p_j^{s_j+1})}(x_i) = 0$ (and hence $F_{(p_j^{k_j})}(x_i) = 0$ for all $k_j > s_j$). If $s_j = t_j$ this will correspond to the case that $F_{(p_j^{k_j})}(x_i) \neq 0$ for all $1 \leq i \leq \ell$ for all k_j , hence why we exclude the element (t_1, \dots, t_n) from \mathcal{S} as this corresponds to the case that there are no zeros, which we treated in Proposition 5.1. With this motivation we will define $J_S = \{j : s_j \neq t_j\}$.

Corollary 5.2. *Let $a_{i,j,k_j} \in \mathbb{F}_q$ such that for m_S of the i we have*

$$a_{i,j,1}, \dots, a_{i,j,s_j} \neq 0 \text{ and } a_{i,j,s_j+1}, \dots, a_{i,j,t_j} = 0, \quad 1 \leq j \leq n$$

for all $S \in \mathcal{S}$. Further if $a_{i,j,k_j} \neq 0$ then $a_{i,j,k_j} = a_{i,j,k_j-1}(b_{i,j,k_j})^{p^{k_j-1}}$ for some $b_{i,j,k_j} \in \mathbb{F}_q^$. Again, we set $a_{i,j,0} = 1$ so that $a_{i,j,1} = b_{i,j,1}$. Then,*

$$\begin{aligned} & |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i) = a_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}| \\ &= \frac{L_{r-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{r-1}} \prod_{S \in \mathcal{S}} \left(\frac{\prod_{j \in J_S} (p_j - 1) p_j^{t_j - s_j} \prod_{j=1}^n p_j^{\frac{s_j(s_j-1)}{2}}}{(q+r-1) \prod_{j=1}^n (q-1)^{s_j}} \right)^{m_S} \\ & \quad \times \left(\frac{q \prod_{j=1}^n p_j^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{T_n} (q+r-1)} \right)^{\ell - \sum_{S \in \mathcal{S}} m_S} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}}\right) \right). \end{aligned}$$

Proof. If we replace $f_{\vec{\alpha}}$ by $f'_{\vec{\alpha}}$, the polynomial divided by its roots, and $F'_{(p_j^{k_j})}$ as the corresponding product of $f'_{\vec{\alpha}}$. $F'_{(p_j^{k_j})}(x_i)$ will be determined by $F_{(p_j^{k_j})}(x_i)$ for $k_j \leq s_j$ and $F'_{(p_j^{k_j})}(x_i)$ will be determined, up to a p^{k_j-1} th root of unity, by $F_{(p_j^{k_j-1})}(x_i)$ for $s_j < k_j \leq t_j$. Summing up over all the necessary partitions of m_S will give the desired result. \square

Note that if we let $d = \prod_{j=1}^n p_j^{s_j}$, then we can write

$$\prod_{j \in J_S} (p_j - 1) p_j^{t_j - s_j} = \phi\left(\frac{r}{d}\right).$$

This illustrates why it was important to consider the set J_S for if the left hand product was over all the j , we would not get this nice equality.

Let $\vec{1} \in \mathcal{R}$ be the element that has 1 in the $T_j + 1$ position $j = 0, \dots, n-1$ and 0 everywhere else. Then set $\mathcal{R}' = \mathcal{R} \setminus \vec{1}$. Define

$$\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})} = \{(f_{\vec{1}}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{d_{\vec{1}}} \times \prod_{\vec{\alpha} \in \mathcal{R}'} \mathcal{F}_{\vec{\alpha}} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \text{ for all } \vec{\alpha} \neq \vec{\beta}\}$$

With this definition, define $\mathcal{F}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}}, \mathcal{F}_{[\vec{d}(\vec{\alpha})]}$ and $\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$ the same way as in Section 4.

Now, if x_{q+1} is the point at infinity, then

$$F_{(p_j^{k_j})}(x_{q+1}) = \begin{cases} \text{leading coefficient of } f_{\vec{1}} & (f_{\vec{\alpha}}) \in \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}^{\vec{\beta}} \\ 0 & \text{otherwise} \end{cases}$$

where $\beta = (\beta_1, \dots, \beta_{T_n}) \in \mathcal{R}$ is any tuple such that $\beta_{T_j+1}, \dots, \beta_{T_j+k_j} = 0$.

Similarly to Corollaries 4.3 and 4.4, we get

Corollary 5.3. *Let $\epsilon_{i,j,k_j} \in \mu_{p_j^{k_j}} \cup \{0\}$ such that for m_S of the i we have*

$$\epsilon_{i,j,1}, \dots, \epsilon_{i,j,s_j} \neq 0 \text{ and } \epsilon_{i,j,s_j+1}, \dots, \epsilon_{i,j,t_j} = 0, \quad 1 \leq j \leq n$$

for all $S \in \mathcal{S}$. Further if $\epsilon_{i,j,k_j} \neq 0$ then $\epsilon_{i,j,k_j} = (\epsilon_{i,j,k_j-1})^p$.

$$\frac{|\{(f_{\vec{\alpha}}) \in \hat{F}_{[\vec{d}(\vec{\alpha})]} : \chi_{p_j^{k_j}}(F_{(p_j^{k_j})}(x_i)) = \epsilon_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq q+1\}|}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|} \\ = \prod_{S \in \mathcal{S}} \left(\frac{\prod_{j \in J_S} (p_j - 1) p_j^{t_j - s_j}}{\prod_{j=1}^n p_j^{s_j} (q + r - 1)} \right)^{m_S} \left(\frac{q}{r(q + r - 1)} \right)^{q+1 - \sum_{S \in \mathcal{S}} m_S} \left(1 + O \left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).$$

Applying this Corollary we obtain

Proof of Theorem 1.2.

$$\frac{|\{(f_{\vec{\alpha}}) \in \hat{F}_{[\vec{d}(\vec{\alpha})]} : S_d(F_d) = M_d, \forall d|r\}|}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|} \\ = \frac{\sum_{\substack{E_{d,1}, \dots, E_{d,q+1} \in \mu_d \cup \{0\} \\ \sum_{i=1}^{q+1} E_{d,i} = M_d \\ E_{d,i} = \prod_{p|d} (E_{p^{v_p(d)}, i})^{\sigma_p \forall d|r} \\ E_{p_j^{k_j}, i} = 0 \implies E_{p_j^{s_j}, i} = 0 \text{ and} \\ E_{p_j^{s_j}, i} \neq 0 \implies E_{p_j^{k_j}, i} = E_{p_j^{s_j-k_j}, i} \quad \forall j, k_j \leq s_j \leq t_j}}}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|} \frac{|\{(f_{\vec{\alpha}}) \in \hat{F}_{[\vec{d}(\vec{\alpha})]} : \chi_d(F_d(x_i)) = E_{d,i}, \forall d|r, 1 \leq i \leq q+1\}|}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|} \\ = \frac{\sum_{\substack{E_{d,1}, \dots, E_{d,q+1} \in \mu_d \cup \{0\} \\ \sum_{i=1}^{q+1} E_{d,i} = M_d \\ E_{d,i} = \prod_{p|d} (E_{p^{v_p(d)}, i})^{\sigma_p \forall d|r} \\ E_{p_j^{k_j}, i} = 0 \implies E_{p_j^{s_j}, i} = 0 \text{ and} \\ E_{p_j^{s_j}, i} \neq 0 \implies E_{p_j^{k_j}, i} = E_{p_j^{s_j-k_j}, i} \quad \forall j, k_j \leq s_j \leq t_j}}}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|} \prod_{S \in \mathcal{S}} \left(\frac{\prod_{j \in J_S} (p_j - 1) p_j^{t_j - s_j}}{\prod_{j=1}^n p_j^{s_j} (q + r - 1)} \right)^{m_S} \\ \times \left(\frac{q}{r(q + r - 1)} \right)^{q+1 - \sum_{S \in \mathcal{S}} m_S} \left(1 + O \left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \\ = \text{Prob} \left(\sum_{i=1}^{q+1} X_{d,i} = M_d \text{ for all } d|r \right) \left(1 + O \left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right)$$

Where in the subscript we have $\sigma_p = p^{-v_p(d)} \pmod{\frac{d}{p^{v_p(d)}}}$.

Further, if we let $d = \prod_{j=1}^n p_j^{s_j}$ then factor being raised to the m_S can be rewritten as

$$\frac{\phi\left(\frac{r}{d}\right)}{d(q+r-1)}$$

and, if $d \neq r$, the $X_{p^s, i}$ satisfy the relationship

$\text{Prob}(X_{p^s, i} = \epsilon_{p^s, i} \neq 0, 1 \leq s \leq v_p(d) \text{ and } X_{p^s, i} = 0, v_p(d) < s \leq v_p(r) \text{ for all } p|r)$

$$= \begin{cases} \frac{\phi\left(\frac{r}{d}\right)}{d(q+r-1)} & \text{if } \epsilon_{p^{s-1}, i} = \epsilon_{p^s, i}^p \text{ for all } p|r, 1 \leq s \leq v_p(d) \\ 0 & \text{otherwise} \end{cases}.$$

If $d = r$, then

$$\text{Prob}(X_{p^s,i} = \epsilon_{p^s,i}, s \leq v_p(r), \text{ for all } p|r) = \begin{cases} \frac{q}{r(q+r-1)} & \text{if } \epsilon_{p^{s-1},i} = \epsilon_{p^s,i}^p, 1 \leq s \leq v_p(r), \text{ for all } p|r \\ 0 & \text{otherwise} \end{cases}.$$

Notice also, since the σ_p come from the Chinese Remainder Theorem, if $X_{d,i} \neq 0$ then the value of $X_{p^{v_p(d)},i}$ is uniquely determined and hence so are $X_{p^k,i}$ for all $p|r$ and $k \leq v_p(d)$. Moreover, for $k > v_p(d)$, $X_{p^k,i}$ will either be 0 or determined, up to a $p^{k-v_p(d)}$ th root of unity. From here we get

$$\begin{aligned} & \text{Prob}(X_{d,i} = \epsilon_{d,i} \neq 0) \\ &= \sum_{\substack{d_1 \\ d|d_1}} \sum' \text{Prob}\left(X_{p^s,i} = \epsilon_{p^{v_p(d_1)},i}^{p^{v_p(d_1)-s}}, 1 \leq s \leq v_p(d_1) \text{ and } X_{p^s,i} = 0, v_p(d_1) < s \leq v_p(r) \text{ for all } p|r\right) \end{aligned}$$

where \sum' is the sum that runs over all

$$\epsilon_{p^{v_p(d_1)},i} \in \mu_{p^{v_p(d_1)}} \text{ such that } \epsilon_{p^{v_p(d_1)},i}^{p^{v_p(d_1)-v_p(d)}} = \epsilon_{p^{v_p(d)},i} \text{ for all } p|r.$$

Hence,

$$\begin{aligned} &= \sum_{\substack{d_1 \neq r \\ d|d_1}} \sum' \frac{\phi\left(\frac{r}{d_1}\right)}{d_1(q+r-1)} + \sum_{d_1=r} \sum' \frac{q}{r(q+r-1)} \\ &= \frac{q + \sum_{\substack{d_1 \neq r \\ d|d_1}} \phi\left(\frac{r}{d_1}\right)}{d(q+r-1)} = \frac{q + \sum_{n|\frac{r}{d}} \phi\left(\frac{r/d}{n}\right) - 1}{d(q+r-1)} = \frac{q + \frac{r}{d} - 1}{d(q+r-1)}. \end{aligned}$$

Therefore

$$\text{Prob}(X_{d,i} = 0) = 1 - \sum_{\epsilon_{d,i} \in \mu_d} \text{Prob}(X_{d,i} = \epsilon_{d,i}) = 1 - \frac{q + \frac{r}{d} - 1}{q+r-1} = \frac{r - \frac{r}{d}}{q+r-1}$$

□

6. HEURISTIC

In this section we will discuss a heuristic for Corollary 5.2 and consequently Theorem 1.2. First we will need Lemma 8.1 from [2].

Lemma 6.1. *Let S_n be the set of n -tuples (F_1, \dots, F_n) of nonzero residues of modulo $(X-t)^2$ such that $(X-t)$ divides at most one of the F_i . Then*

$$|S_n| = q^{n-1}(q-1)^n(q+n).$$

The set S models the set of n squarefree coprime polynomials. Write $F = f_1 f_2^2 \dots f_{r-1}^{r-1}$ with $(f_1, \dots, f_{r-1}) \in S_{r-1}$. If $r = \prod_{j=1}^n p_j^{t_j}$ then Corollary 5.2 deals with $F_{(p_j^{k_j})}$ for $1 \leq j \leq n$, $1 \leq k_j \leq t_j$. That is, we want to determine how many $(r-1)$ -tuples there are in S_{r-1} that satisfy

$$F_{(p_j^{k_j})} \equiv a_{j,k_j} \pmod{(X-t)^2}$$

where $a_{j,k_j} = a_{j,k_j-1}(b_{j,k_j})^{p_j^{k_j-1}}$ for some b_{j,k_j} .

Suppose $a_{j,t_j} \not\equiv 0 \pmod{(X-t)}$ for all j . Using the notation $F_{(p_j^{k_j})} = \prod_{i=1}^{r-1} f_i^i \pmod{p_j^{k_j}}$ we will start with $j = 1$. The condition of

$$F_{(p_1)} \equiv a_{1,1} \pmod{(X-t)^2}$$

says that there are $(q(q-1))^{r-\frac{r}{p_1}-1}$ choices for f_i with $i \neq 1$ and q choices for f_1 which gives a total of $q^{r-\frac{r}{p_1}}(q-1)^{r-\frac{r}{p_1}-1}$ choices of the f_i . Now if we fix one of these choices and look at

$$F_{(p_1^2)} \equiv a_{1,2} = a_{1,1}(b_{1,2})^p \pmod{(X-t)^2}$$

then there would be $(q(q-1))^{\frac{r}{p_1}-\frac{r}{p_1^2}-1}$ choices for the $f_{p_1 i}$ with $i \neq 1$ and $p_1 q$ choices for f_{p_1} which gives a total of $p_1 q^{r-\frac{r}{p_1^2}}(q-1)^{r-\frac{r}{p_1^2}-2}$. From here we can see that if we consider all the conditions

$$F_{(p_1^{k_1})} \equiv a_{1,k_1} \pmod{(X-t)^2} \quad 1 \leq k_1 \leq t_1$$

we will get $p_1^{\frac{t_1(t_1-1)}{2}} q^{r-\frac{r}{p_1^{t_1}}}(q-1)^{r-\frac{r}{p_1^{t_1}}-t_1-1}$. Now, if we fix these choices and look at

$$F_{(p_2)} \equiv a_{2,1} \pmod{(X-t)^2}$$

then all the f_i appearing in $F_{(p_2)}$ such that $i \not\equiv 0 \pmod{p_1^{t_1}}$ are already determined.

If we let $j = p_1^{-t_1} \pmod{\frac{r}{p_1^{t_1}}}$ then there are $(q(q-1))^{\frac{r}{p_1}-\frac{r}{p_1^{t_1} p_2}-1}$ choices for the $f_{p_1^{t_1} i}$ such that $i \neq j$, $i \not\equiv 0 \pmod{p_2}$ and q choices for $f_{p_1^{t_1} j}$. Therefore we get a total of $p_1^{\frac{t_1(t_1-1)}{2}} q^{r-\frac{r}{p_1^{t_1} p_2}}(q-1)^{r-\frac{r}{p_1^{t_1} p_2}-t_1-1}$. From here it is clear what will happen and if we look at all the conditions

$$F_{(p_j^{k_j})} \equiv a_{j,k_j} \pmod{(X-t)^2} \quad 1 \leq k_j \leq t_j, 1 \leq j \leq n$$

then we get

$$(q(q-1))^{r-1} \prod_{j=1}^n \frac{p_j^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{t_j}}.$$

Dividing by $|S|$, we get

$$\frac{q}{q+r-1} \prod_{j=1}^n \frac{p_j^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{t_j}}$$

which is consistent with Proposition 5.1.

Now suppose that not all a_{i,j,k_j} are non-zero. As with the statement of Corollary 5.2 we have s_1, \dots, s_n such that $0 \leq s_j \leq t_j$ (but not all $s_j = t_j$) and $a_{j,k_j} \equiv 0 \pmod{(X-t)}$ if and only if $k_j > s_j$, $j = 1, \dots, n$. Let $d = \prod_{j=1}^n p_j^{s_j}$ then, as above, the conditions

$$F_{(p_j^{k_j})} \equiv a_{j,k_j} \pmod{(X-t)^2} \quad 1 \leq k_j \leq s_j, j = 1, \dots, n$$

yields

$$(q(q-1))^{r-d} \prod_{j=1}^n \frac{p_j^{\frac{s_j(s_j-1)}{2}}}{(q-1)^{s_j}}$$

choices of the f_i . Fixing one of these choices, consider the conditions

$$F_{(p_j^{s_j+1})} \equiv a_{j,s_j+1} \pmod{(X-t)^2} \quad j = 1, \dots, n \text{ such that } s_j \neq t_j.$$

The value of f_i is already determined if $i \not\equiv 0 \pmod{d}$. Further there is exactly one $1 \leq i \leq r-1$ such that $v_{p_j}(i) = s_j$ for all $1 \leq j \leq n$ such that $f_i \equiv 0 \pmod{(X-t)}$. Then f_i has $(q-1)$ different choices and the rest of the f_j have $(q(q-1))^{\frac{r}{d}-\frac{r}{d'}-1}$ different choices where

$$d' = \prod_{\substack{j=1 \\ s_j \neq t_j}}^n p_j^{s_j+1} \prod_{\substack{j=1 \\ s_j = t_j}}^n p_j^{t_j}.$$

Moreover, there are $\phi(\frac{r}{d}) = \prod_{j=1, s_j \neq t_j}^n (p_j-1)p_j^{t_j-s_j-1}$ such i that satisfy $v_{p_j}(i) = s_j$ for all $1 \leq j \leq n$. Hence with the new conditions there are

$$q^{r-\frac{r}{d'}-1}(q-1)^{r-\frac{r}{d'}} \phi\left(\frac{r}{d}\right) \prod_{j=1}^n \frac{p_j^{\frac{s_j(s_j-1)}{2}}}{(q-1)^{s_j}}$$

choices of the f_i .

For the remaining $\frac{r}{d'}-1$ of the f_i not accounted for, the conditions

$$F_{(p_j^{k_j})} \equiv a_{j,k_j} \pmod{(X-t)^2} \quad k_j > s_j+1, j = 1, \dots, n \text{ such that } s_j \neq t_j$$

are already satisfied as $a_{j,k_j} \equiv 0 \pmod{(X-t)}$. Therefore, we need only $f_i \not\equiv 0 \pmod{(X-t)}$ giving $(q(q-1))^{\frac{r}{d'}-1}$ choices. Therefore our final count will be

$$q^{r-2}(q-1)^{r-1} \phi\left(\frac{r}{d}\right) \prod_{j=1}^n \frac{p_j^{\frac{s_j(s_j-1)}{2}}}{(q-1)^{s_j}}.$$

Dividing by $|S|$ gives

$$\frac{\phi\left(\frac{r}{d}\right)}{q+r-1} \prod_{j=1}^n \frac{p_j^{\frac{s_j(s_j-1)}{2}}}{(q-1)^{s_j}}$$

which is consistent with Corollary 5.2.

Acknowledgements: I would like to thank Chantal David for the many discussions we had about this topic and for taking time to make sure the final paper was presentable. I would also like to thank Elisa Lorenzo, Giulio Meleleo and Piermarco Milione for their helpful discussions about their paper.

REFERENCES

- [1] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalin, *Biased statistics for traces of cyclic p -fold covers over finite fields*, WIN–Women in Numbers: Research Directions in Number Theory **60** (2009), 121–143.
- [2] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalin, *Statistics for traces of cyclic trigonal curves over finite fields*, International Mathematics Research Notices (2009), rnp162.
- [3] Nicholas M Katz and Peter Sarnak, *Random matrices, frobenius eigenvalues, and monodromy*, vol. 45, American Mathematical Soc., 1999.
- [4] Pär Kurlberg and Zeév Rudnick, *The fluctuations in the number of points on a hyperelliptic curve over a finite field*, Journal of Number Theory **129** (2009), no. 3, 580–587.
- [5] Elisa Lorenzo, Giulio Meleleo, and Piermarco Milione, *Statistics for biquadratic covers of the projective line over finite fields*, arXiv preprint arXiv:1503.03276 (2015).
- [6] Michael Rosen, *Number theory in function fields*, vol. 210, Springer Science & Business Media, 2013.